SYSTEM SECURITY

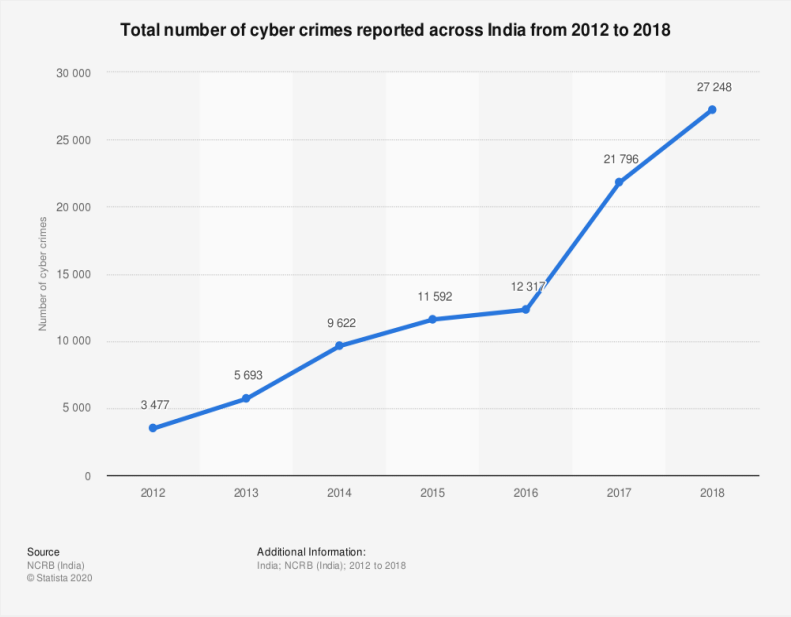
By Prof. Krishna Samdani

INTRODUCTION

- Basic Components of Computer Security (CIA) / Goals of Security
- Vulnerabilities
- Threats
- Attacks
- Controls
- Computer Criminals

NEED OF SYSTEM SECURITY

All organizations make use of the network to work efficiently. They utilize the network by gathering, processing, storing and sharing the information. Thus cyber/system security is the *efforts of safe guarding this digital information* at personal or corporate level.

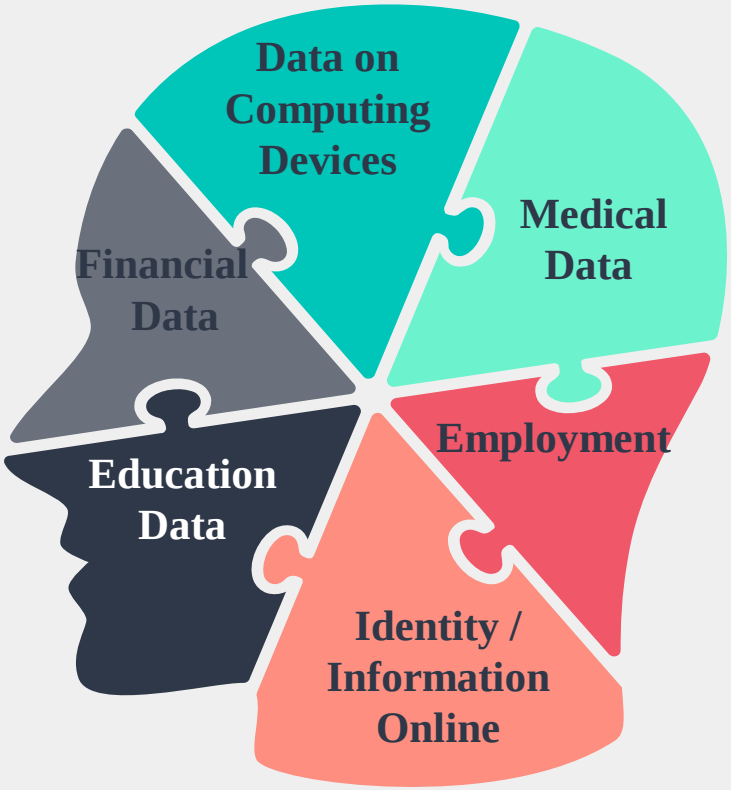


TYPES OF IDENTITY

- **Offline**
  - Offline identity is what your family and friends know about you like name, age, address etc.
- **Online**
  - Online identity is what you pretend to be.

DATA

- Any information about you is your data
- This data is used to identify you online
- Your computing devices have become the portal to your data and generate information about you
- Hackers want your money - that's a *short term profit*
- Hackers want your identity - that a *long term profit*



GOALS OF SECURITY

- **Confidentiality**
  - Only intended users should be able to access the contents of a message
- **Integrity**
  - A message should be preserved as it travels from one point to another
- **Availability**
  - It ensures that the resources are available to the authorized entities at all time
- **Authentication**
  - Assuring that the communicating entity is the one that it claims to be
- **Access Control**
  - Who can access what resources and under what conditions
- **Non-Repudiation**
  - Protection against denial by one of the entities involved in a communication

TERMINOLOGIES

Vulnerability

- It's a weakness in the system that might be exploited to cause loss or harm

E.g.: *System may be vulnerable to unauthorized data manipulation.*

Threats

- It is a set of circumstances that has potential to cause loss or harm
- It can be human-initiated and computer-initiated ones, natural disasters.

E.g.: *Internal employee can be a threat to the organisation*

Attacks

- An attempt to evade security services & violate the security policy of a system

E.g.: *DDoS attack on the server or system*

VULNERABILITY

- The basic questions regarding to security that can arise in our mind are-
  1. Why attackers attack our system?
  2. Is there any weak component present in our system?
  3. What are the precautions we need to take against attack?
- Vulnerability is nothing but the *weakness in the system*. Weakness in the system may exploit an attack. Weakness can be in coding, design or can be anything related to software development.
- Types :
  1. Hardware Vulnerability
  2. Software Vulnerability
  3. Data Vulnerability

THREATS

- A threat is a potential for violation of security or a possible danger that might exploit vulnerability.
- In other words a threat is a set of activity that has ability to cause harm. The threat can be either generated by Human or Computer.
- Threat is purposely created by an attacker to attack on the system. In other words, an exploitation of vulnerability is attack on the system.
- There are four kinds of threats possible: *Interception, Interruption, Modification, and Fabrication*

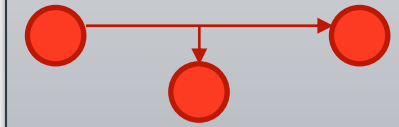
TYPES OF THREATS

Interruption

- In interruption, the data may be lost or unavailable due to some unauthorized party

Interception

- Interception is keeping track of traffic without modification. In other words, some unauthorized system has gained access to an asset.

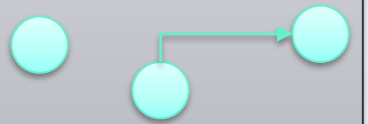


Modification

- In modification, data is modified in some way. Receiver doesn't have any knowledge of this modification

Fabrication

- In fabrication, attacker might hide his own identity and can send the data to receiver from some trusted host.



ATTACKS

- An exploitation of vulnerability is attack on the system
- *The threat in action* is called as Attack

Passive Attacks

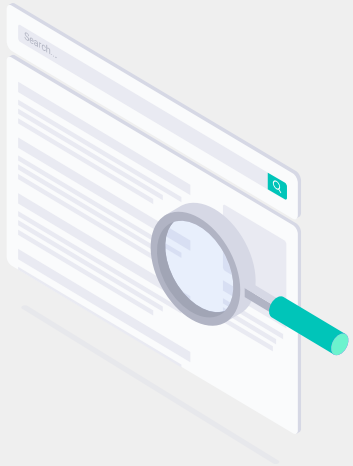
Goal to obtain information

- ***Release of message contents***
- ***Traffic analysis***

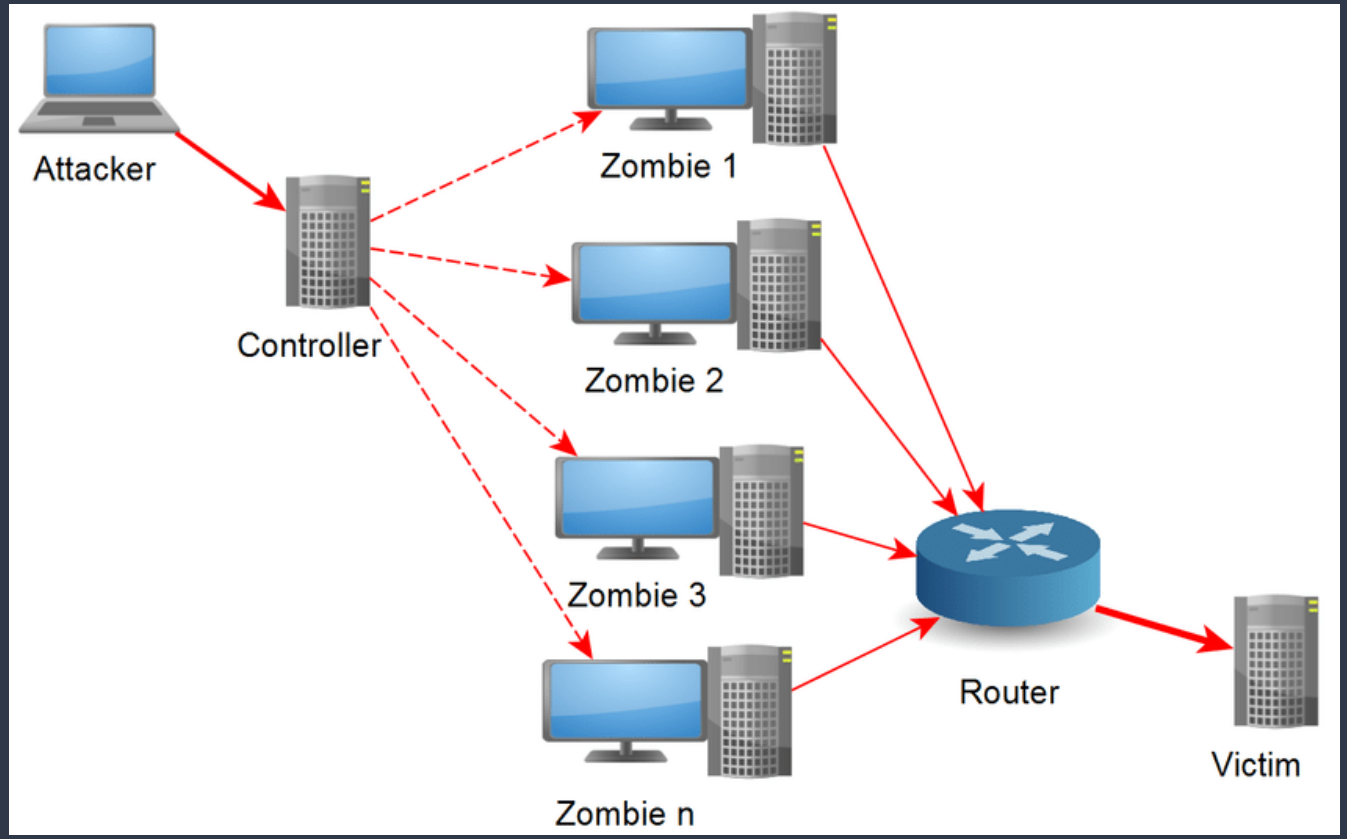
Active Attacks

Attempts to alter system resources or affect their operation

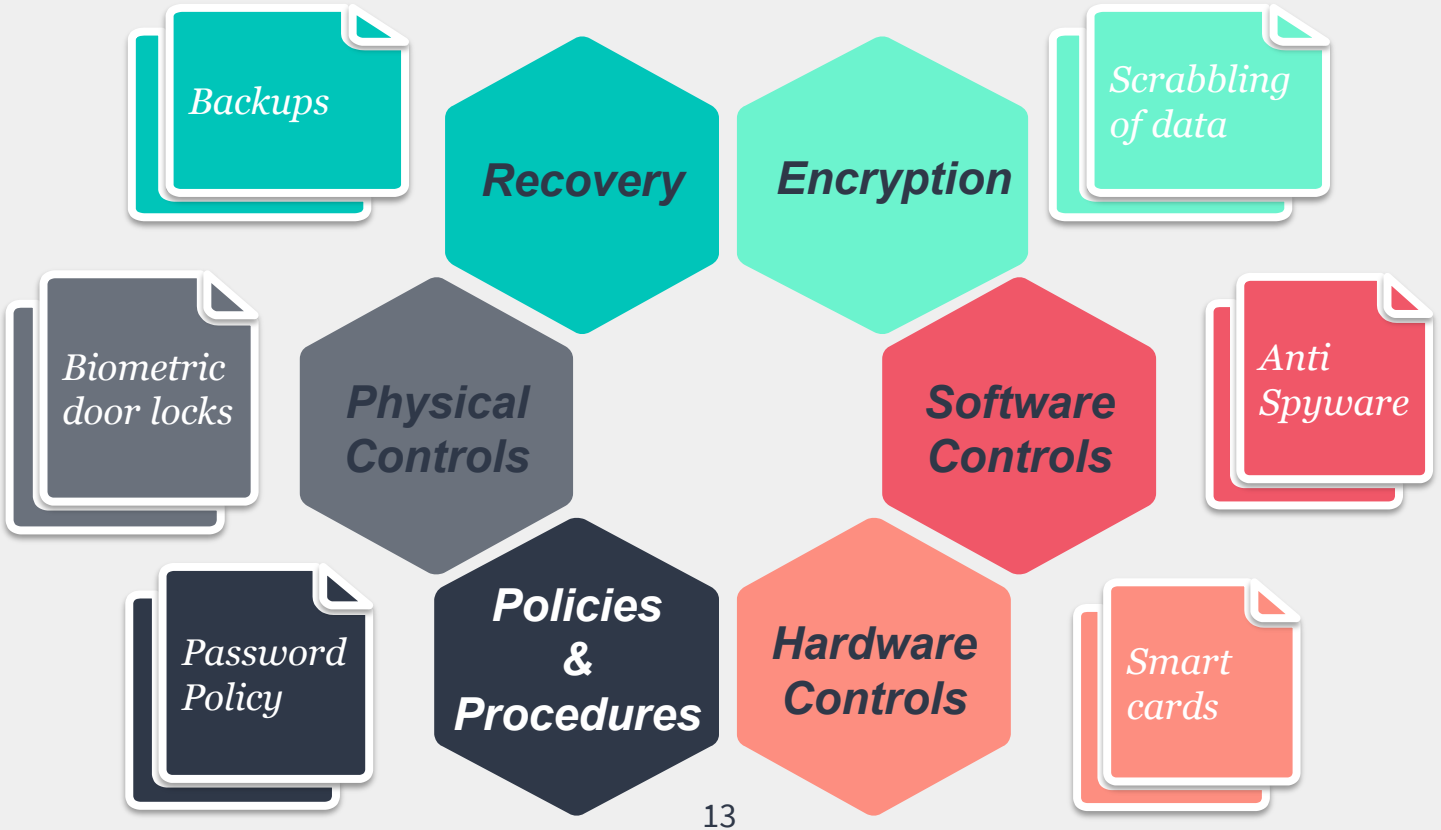
- ***Masquerade***
- ***Replay***
- ***Modifications of messages***
- ***Denial of Service***



DDOS ATTACKS



SECURITY CONTROLS



COMPUTER CRIMINALS

1. **Amateurs**
   - Normal people, who observes the weakness in a security system that allows them to access cash or other valuables….
2. **Crackers or malicious hackers**
   - Attack for curiosity, personal gain or self satisfaction
3. **Career Criminals**
   - Understand the targets of computer crime.
4. **Terrorists**
   - Targets of attack: denial-of-service
   - Other methods of attack

INTERNET STANDARDS AND RFC

- Internet standard is a special Request for Comments (RFC) or set of RFCs.
- An RFC that is to become a Standard or part of a Standard begins as an Internet Draft, and is later (usually after several revisions) accepted and published by the RFC Editor as a RFC and labeled a *Proposed Standard*
- Later, an RFC is labeled a *Draft Standard*, and finally a *Standard*.
- The *RFC Editor* assigns each RFC a *unique serial number*. Once assigned a number and published, an RFC is *never cancelled or modified*; if the document requires amendments, the authors publish a revised document.

STUDY MATERIALS

- Matt Bishop,“ Introduction to Computer Security ”, Pearson Education,2005.

Please Note : PPT’s are for Reference Only , NOT AS A STUDY MATERIAL

Contact

Krishna Samdani

krishna.samdani@nmims.edu

Mobile- 9920407045

Seating – 1A Faculty Area MPSTME Building

Thanks!

Any questions?